Lab 1 – TCP Attacks - Concepts

CS 6823 –Network Security
Look forward to Lesson 3

Phillip Mak
pmak@nyu.edu

Lab 1 Overview

- Task 1: SYN Flood Attacks
  - Test telnet during a SYN Flood, with SYN Flood protections ON and OFF
    - There are two SYN Flood protection methods:
      - SYN Cookies
      - Reserve TCP Connections for “proven destinations”

- Task 2: TCP RST Attack
  - Guess the correct SEQ/ACK Number to perform a RST Attack
  - 5% bonus for fully automating the attack

- Task 3: TCP Session Hijacking
  - Guess the correct SEQ/ACK, 5% for automating the attack

- Task 4:
  - Reverse shell. Same as Task 3, but add a reverse shell exploit

SYN Flood Attacks

Connection flooding: Overwhelming connection queue w/ SYN flood

Recall client sends SYN packet with initial seq. number when initiating a connection.

TCP on server machine allocates memory on its connection queue, to track the status of the new half-open connection.

For each half-open connection, server waits for ACK segment, using a timeout that is often > 1 minute

Attack: Send many SYN packets, filling connection queue with half-open connections.

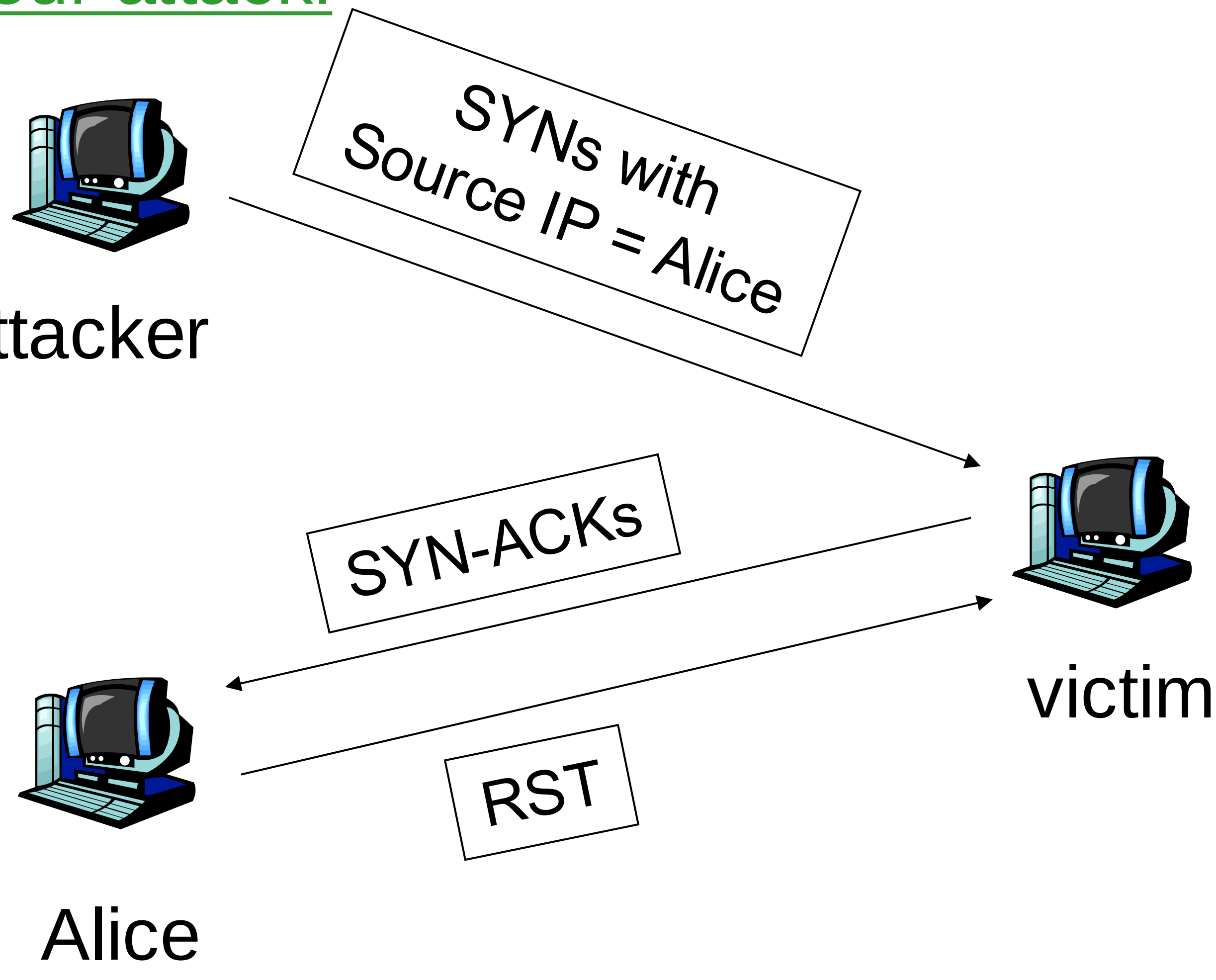
Can spoof source IP address!

When connection queue is exhausted, no new connections can be initiated by legit users.

Need to know of open port on victim’s machine: Port scanning.

DoS: Overwhelming connection queue with SYN flood

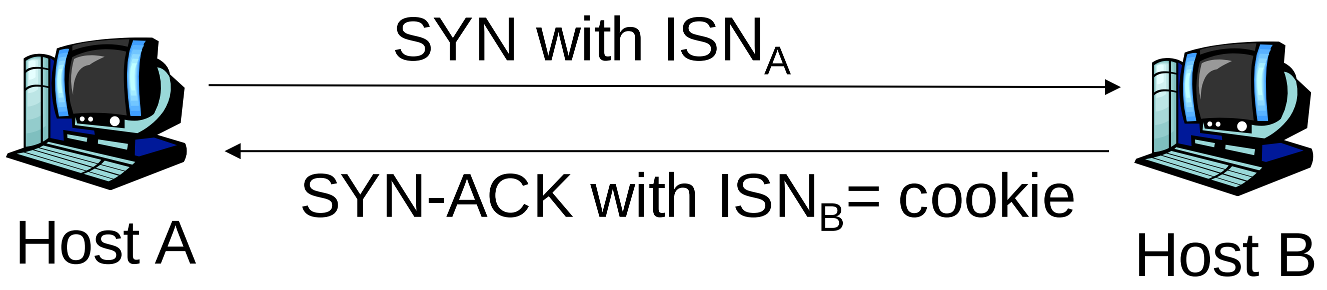
amateur attack:



Connection queue freed up with RST segment

Expert attack: Use multiple source IP addresses, each from unresponsive addresses.

SYN flood defense: SYN cookies (1)



- When SYN segment arrives, host B calculates function (hash) based on:
  - Apache example: Source and destination IP addresses and port numbers, and a secret number
- Host B uses resulting “cookie” for its initial seq # (ISN) in SYNACK
- Host B does not allocate anything to half-open connection:
  - Does not remember A’s ISN
  - Does not remember cookie

SYN flood defense: SYN cookies (2)

If SYN is legitimate
Host A returns ACK

Host B computes same function, verifies function = ACK # in ACK segment
Host B creates socket for connection

Legit connection established without the need for half-open connections

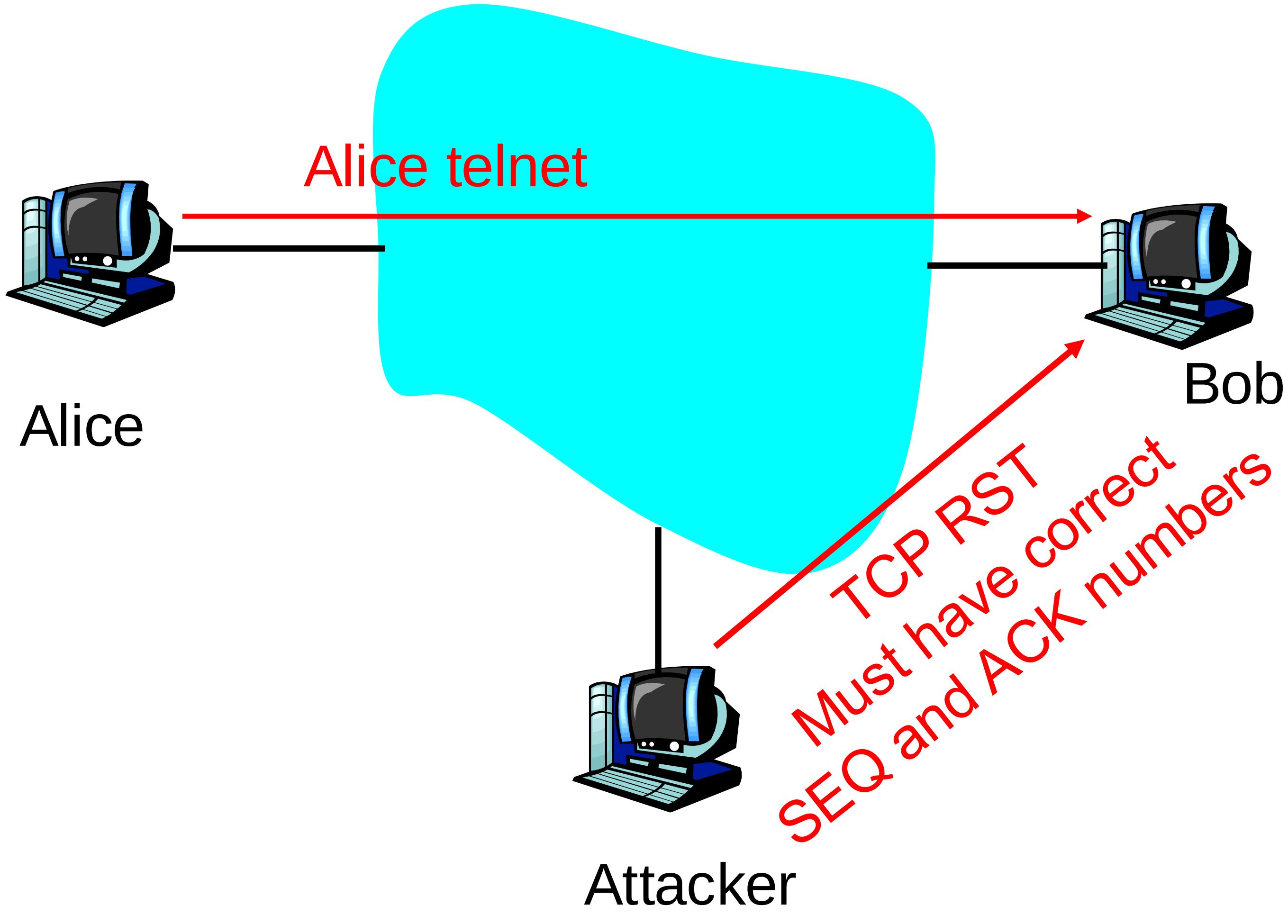
If SYN-flood attack with spoofed IP address
No ACK comes back to B for connection.

No problem: B is not waiting for an ACK

TCP RST Attack

TCP RST Attack

Hint: use the last SEQ/ACK #
For the TCP RST.
The TCP RST attack is either the SEQ or ACK only



- Attacker can break the TCP connection by sending a TCP RST
- Must match the SEQ and ACK Numbers

Q2: Exercise #2

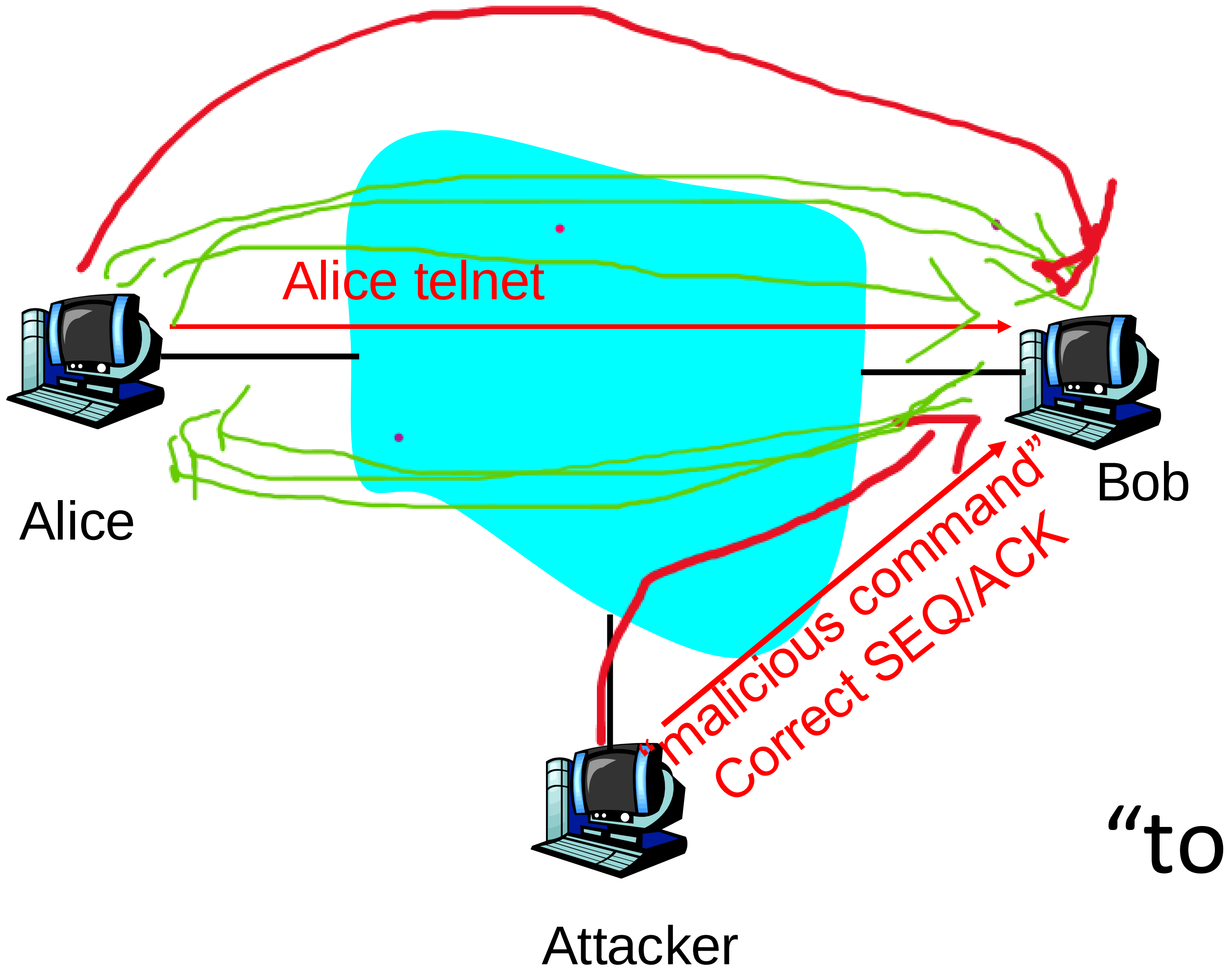
Q2: What happens when a TCP RST attack is sent with the wrong SEQ/ACK # to the target?

TCP Session Hijacking

Hint: take last SEQ/ACK
Use the same SEQ/ACK or use opposite (SEQ=ACK/ACK=SE

Session hijacking

- Take control of one side of a TCP connection
- Marriage of sniffing and spoofing

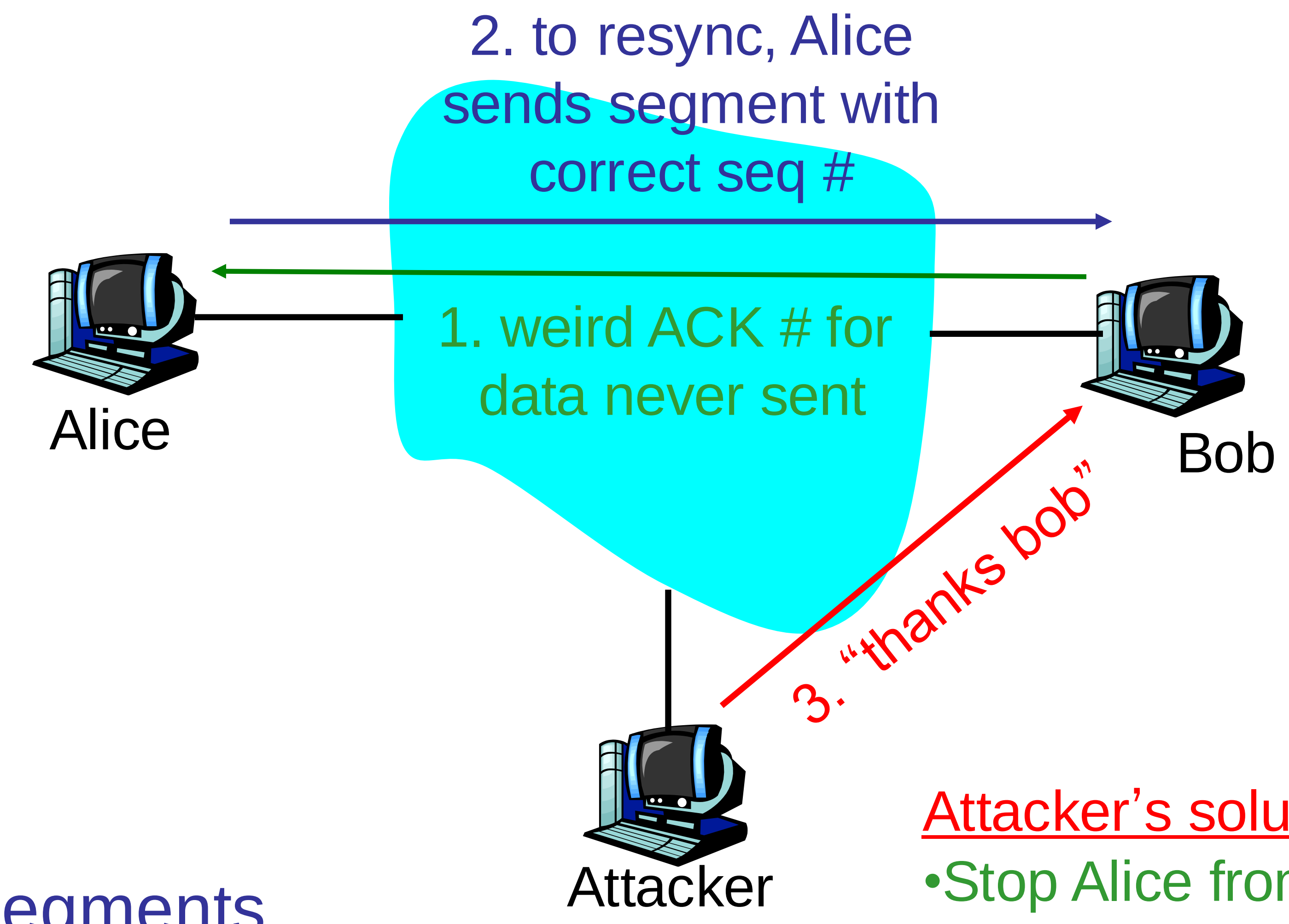


"touch virus.txt"

Session hijacking: The details

- Attacker is on segment where traffic passes from Alice to Bob
  - Attacker sniffs packets
  - Sees TCP packets between Bob and Alice and their sequence numbers
- Attacker jumps in, sending TCP packets to Bob; source IP address = Alice’s IP address
  - Bob now obeys commands sent by attacker, thinking they were sent by Alice
- Principal defense: encryption w/ auth protocol
  - Attacker does not have keys to encrypt and insert meaningful traffic

Session hijacking: limitation


2. to resync, Alice sends segment with correct seq #
1. weird ACK # for data never sent
Alice
Bob
3. "thanks bob"
Attacker

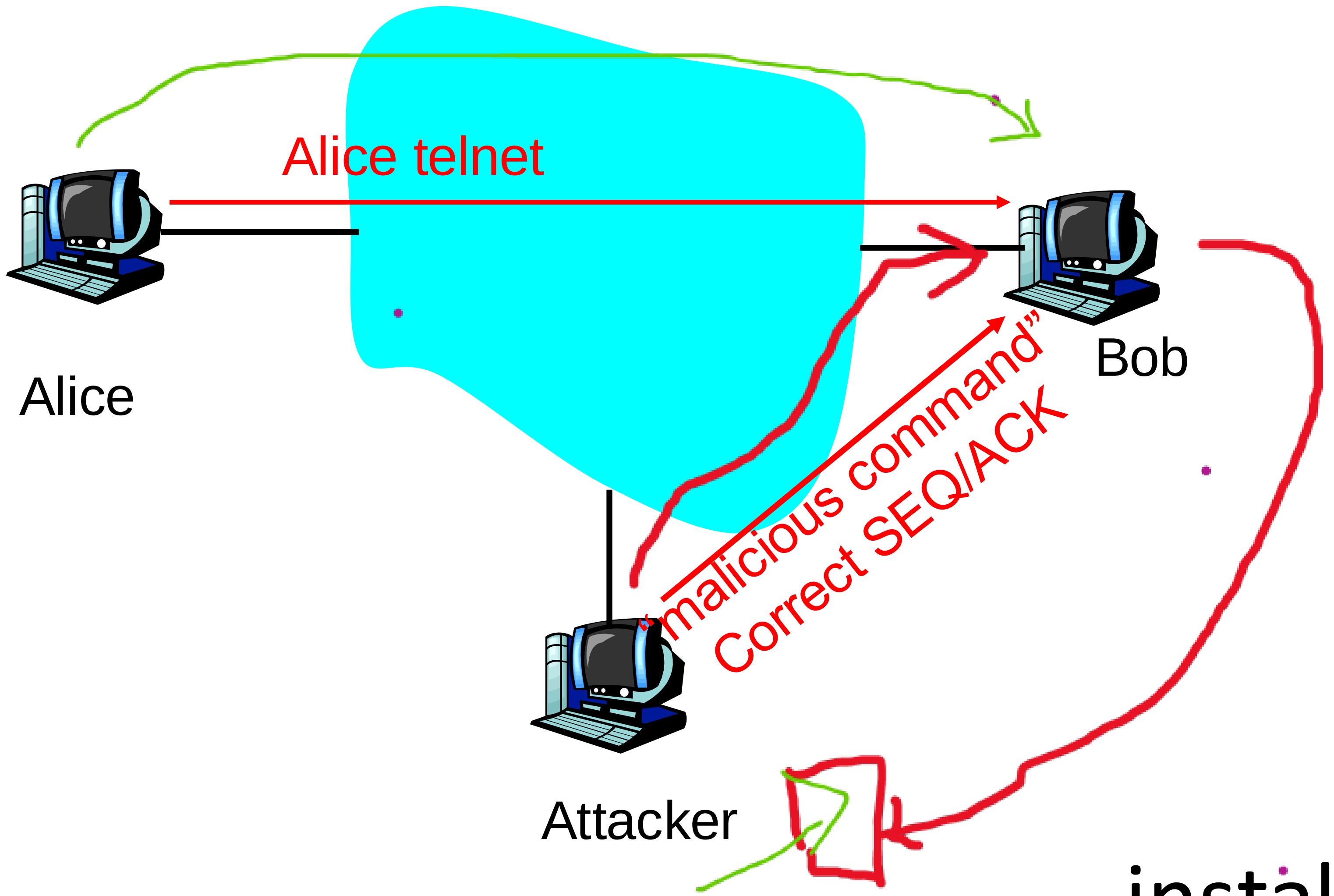
Bob is getting segments from attacker and Alice. Source IP address same, but seq #'s different. Bob likely drops connection.

Attacker's solution:

- Stop Alice from communicating with Bob
- Poison the ARP Cache
  - Send unsolicited ARP replies to Alice and Bob with non-existent MAC addresses
  - Overwrite IP-to-MAC ARP tables so Alice's segments will not reach Bob and vice-versa
  - But attacker continues to hear Bob's segments, communicates with Bob

Task 4: Reverse shell

- Take control of one side of a TCP connection
- Marriage of sniffing and spoofing



install malware